UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
INFORMATION ASSOCIATED WITH THE CELLULAR DEVICE ASSIGNED CALL NUMBER [redacted] THAT IS STORED AT PREMISES CONTROLLED BY AT&T Mobility

Case No. 4:20 MJ 1096 JMB

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the SOUTHERN District of FLORIDA, there is now concealed *(identify the person or describe the property to be seized):*

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Section 1341	Mail Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Mickey Owens

Applicant's signature

Mickey Owens, Task Force Officer, FBI

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 4/30/2020

Judge's signature

City and state: St. Louis, MO

John M. Bodenhausen U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR DEVICE ASSIGNED CALL NUMBER [redacted], THAT IS STORED AT PREMISES CONTROLLED BY **AT&T Mobility**	Case No. 4:20 MJ 1096 JMB **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Federal Bureau of Investigation (FBI) Task Force Officer (TFO) Mickey Owens, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 for information associated with a certain cellular telephone assigned call number [redacted] (hereinafter "the subject phone"), that is stored at premises controlled by **AT&T Mobility** (hereinafter "the Provider"), a wireless telephone service provider headquartered at **AT&T National Compliance Center, 11760 US Highway One Mailstop: Suite 600, North Palm Beach, FL 33408**. The information to be searched is described in the following paragraphs and in Attachment A. The requested warrant would require the Provider to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), and have been since December 3, 2019. I have been a Police Officer for 34 years having completed 900 hours of basic police training and hundreds of hours of ongoing training in community policing and criminal investigations. I am employed by the St. Louis Metropolitan

Police Department and have been so for the last 25 years. I have served 16 years in the criminal investigations unit, including eight years investigating crimes against children and eight years supervising sex crimes investigations. Many of these investigations included obtaining court orders / search warrants for electronic devices, including cell-site information.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 1341 have been committed, are being committed, and will be committed by [redacted] or other persons known and unknown. There is also probable cause to search the location described in Attachment A for the information described in Attachment B for evidence of these crimes.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the District Court for the Eastern District of Missouri is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO WIRELESS PROVIDERS

6. In my training and experience, I have learned that the Provider is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site

data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (*i.e.*, antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (*i.e.*, faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

7. Based on my training and experience, I know that wireless providers can collect cell-site data about the subject phone. I also know that wireless providers such as typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

8. Based on my training and experience, I know that wireless providers typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the subject phone's user or users and may assist in the identification of

co-conspirators and/or victims.

9. Because the cellular device generally attempts to communicate with the closest unobstructed tower, by reviewing the above-described information, your affiant and other law enforcement officers can determine the approximate geographic area from which the communication originated or was received.

10. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

11. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service used, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the

services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates and times of payments and the means and source of payment (including any credit card or bank account number).

PROBABLE CAUSE

12. [redacted] is a Police Officer with the St. Louis Metropolitan Police Department who is approved to work secondary employment for City Wide Security. At City Wide Security [redacted] was directed to patrol the Tower Grove South Neighborhood in a company owned security vehicle which was equipped with a GPS tracking system. As [redacted] would report for his secondary employment at City Wide Security, he was to turn on the security vehicle's ignition which would activate the GPS tracking system and begin to collect data.

13. An investigation revealed that between January 1, 2017 and December 31, 2019 [redacted] requested specific dates to work secondary employment for City Wide Security. [redacted] scheduled his secondary employment with City Wide online, via the internet. City Wide Security scheduled [redacted] to patrol the Tower Grove South Neighborhood on those requested dates, and paid [redacted] for purportedly working those shifts. City Wide Security is paid by the Tower Grove South Neighborhood Association which receives funding from the "Tower Grove South Special Business District" which imposes a tax upon the property owners within the "Special Business District."

14. An audit of the GPS tracking system data from the City Wide Security vehicle assigned to [redacted] discovered no GPS data on the specific dates that [redacted] was scheduled to patrol and for which he was paid for purportedly working. Based upon the fact that the GPS system for that vehicle contained data for other officers that patrolled before and after [redacted]

shift and no reports that the GPS system failed, it is believed that [redacted] did not show up for his shifts, provided false information to City Wide Security and, based upon that false information, [redacted] was paid by City Wide Security by bank checks mailed to him through the United States Postal Service. [redacted] was scheduled to be patrolling on specific dates in the Tower Grove South Neighborhood between January 1, 2017 and December 31, 2019, however no GPS data from the City Wide Security vehicle assigned for [redacted] use exists to verify Stephens started or patrolled in the City Wide Security vehicle on those dates for which he was subsequently paid for. It is believed that [redacted] committed mail fraud by scheming to defraud City Wide Security and by obtaining funds from City Wide Security based upon his false representations. Upon information and belief, cell-site data which might be available for Stephens's known cellular telephone, number [redacted], on the dates Stephens was scheduled to work for City Wide Security, may provide evidence of the alleged federal criminal conduct.

15. [redacted] provided his personal cellular phone number to both the St. Louis Metropolitan Police Department and City Wide Security as [redacted], with the provider identified as **AT&T Mobility**.

AUTHORIZATION REQUEST
INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

16. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41. The United States will execute this warrant by serving the warrant on the Provider. Because the warrant will be served on the Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

17. I further request that the Court direct the Provider to disclose to the United States

any information described in Section I of Attachment B that is within its possession, custody, or control.

REQUEST FOR SEALING

18. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

I state under the penalty of perjury that the foregoing is true and correct.

Mickey Owens, Task Force Officer
Federal Bureau of Investigation

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on April 30th, 2020.

JOHN M. BODENHAUSEN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number [redacted], that are stored at premises controlled by **AT&T Mobility** ("the Provider"), headquartered at **AT&T National Compliance Center, 11760 US Highway One Mailstop: Suite 600, North Palm Beach, FL 33408**.

Attachment B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period January 1, 2017 and December 31, 2019:

a. The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"));

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received as well as per-call measurement data (also known as the "real-time tool" or "RTT" data).

The Provider is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.

II. Information to be Seized by the United States

All information described above in Section I that constitutes evidence of violations of Title 18 U.S.C. § 1341 involving [redacted] during the period June 1, 2017 and August 31, 2019.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **AT&T Mobility**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **AT&T Mobility**. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **AT&T Mobility**, and they were made by **AT&T Mobility** as a regular practice; and

b. such records were generated by **AT&T Mobility's** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **AT&T Mobility** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **AT&T Mobility**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature